



⑮ **BUNDESREPUBLIK  
DEUTSCHLAND**



**DEUTSCHES  
PATENT- UND  
MARKENAMT**

⑩ **Gebrauchsmusterschrift  
DE 200 16 746 U 1**

⑤ Int. Cl. 7:  
**G 06 F 17/30**

⑳	Aktenzeichen:	200 16 746.4
㉔	Anmeldetag:	28. 9. 2000
④	Eintragungstag:	21. 12. 2000
④	Bekanntmachung im Patentblatt:	25. 1. 2001

**DE 200 16 746 U 1**

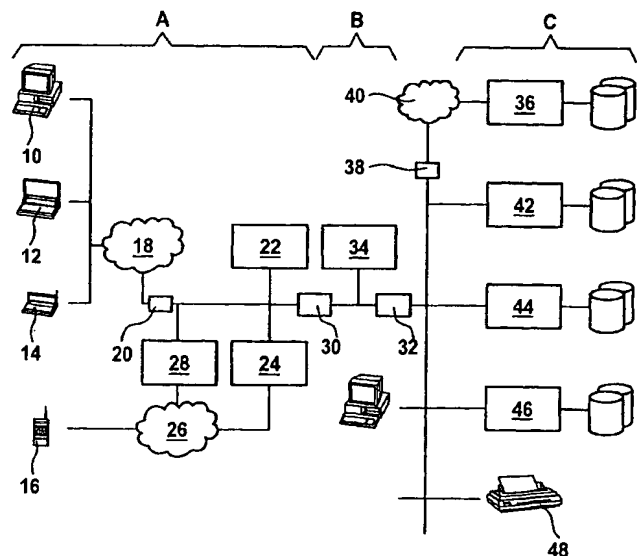
⑥ Innere Priorität:  
100 03 440. 3      27. 01. 2000

⑦ Inhaber:  
Andersen Consulting Unternehmensberatung  
GmbH, 65843 Sulzbach, DE

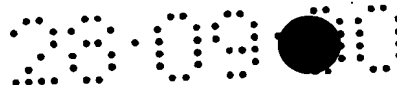
⑦ Vertreter:  
BOEHMERT & BOEHMERT, 28209 Bremen

⑤ Informationsdienstsystem

- ⑤ Informationsdienstsystem mit Applikationseinrichtungen, insbesondere für die Polizei, mit
- Informationssystemen (C),
  - einem intelligenten, dynamisch realisierten Portal (B) für einen einheitlichen Zugang zu den nachgelagerten Informationssystemen (C) mit einem vom Benutzer abhängigen Umfang,
  - mindestens einem Endgerät (10; 12; 14; 16) für einen Zugang zu dem Portal (B), und
  - mindestens einer Kommunikationseinrichtung (17) zum Verbinden des Endgeräts (10, 12, 14, 16) mit dem Portal.



**DE 200 16 746 U 1**



# BOEHMERT & BOEHMERT ANWALTSSOZietät

Boehmert & Boehmert • P.O.B. 10 71 27 • D-28071 Bremen

Deutsches Patent- und Markenamt  
Zweibrückenstr. 12  
80297 München

DR.-ING. KARL BOEHMERT, PA (1899-1973)  
DIPL.-ING. ALBERT BOEHMERT, PA (1902-1993)  
WILHELM I. H. STAHLBERG, RA, Bremen  
DR.-ING. WALTER HOORMANN, PA\*, Bremen  
DIPL.-PHYS. DR. HEINZ GODDAR, PA\*, München  
DR.-ING. ROLAND LIESEGANG, PA\*, München  
WOLF-DIETER KUNTZE, RA, Bremen, Alicante  
DIPL.-PHYS. ROBERT MÜNZHUBER, PA (1933-1992)  
DR. LUDWIG KOUKER, RA, Bremen  
DR. (CHEM.) ANDREAS WINKLER, PA\*, Bremen  
MICHAELA HUTH-DIERIG, RA, München  
DIPL.-PHYS. DR. MARION TÖNHARDT, PA\*, Detmold  
DR. ANDREAS EBERT-WEIDENFELLER, RA, Bremen  
DIPL.-ING. EVA LIESEGANG, PA\*, München  
DR. AXEL NORDEMANN, RA, Berlin  
DIPL.-PHYS. DR. DOROTÉE WEBER-BRULS, PA\*, Frankfurt  
DIPL.-PHYS. DR. STEFAN SCHOHE, PA\*, München  
DR.-ING. MATTHIAS PHILIPP, PA\*, Bielefeld  
DR. JAN BERND NORDEMANN, LL.M., RA, Berlin

PROF. DR. WILHELM NORDEMANN, RA, BRB\*  
DIPL.-PHYS. EDUARD BAUMANN, PA\*, Höhenkirchen  
DR.-ING. GERALD KLÖPSCH, PA\*, Düsseldorf  
DIPL.-ING. HANS W. GROENING, PA\*, München  
DIPL.-ING. SIEGFRIED SCHIRMER, PA\*, Bielefeld  
DIPL.-PHYS. LORENZ HANEWINKEL, PA\*, Paderborn  
DIPL.-ING. DR. JAN TÖNNIES, PA, RA, Kiel  
DIPL.-PHYS. CHRISTIAN BIEHL, PA\*, Kiel  
MARTIN WIRTZ, RA, Detmold  
DR. DETMAR SCHÄFER, RA, Bremen  
DIPL.-PHYS. DR.-ING. UWE MANASSE, PA\*, Bremen  
DR. CHRISTIAN CZYCHOWSKI, RA, Berlin  
DR. CARL-RICHARD HAARMANN, RA, München  
DIPL.-PHYS. DR. THOMAS L. BITTNER, PA\*, Berlin  
DR. VOLKER SCHMITZ, RA, München  
DR. FRIEDRICH NICOLAUS HEISE, RA, Potsdam  
DIPL.-PHYS. CHRISTIAN W. APPELT, PA, München  
DR. ANKE NORDEMANN-SCHIFFEL, RA\*, Potsdam  
KERSTIN MAUCH, LL.M., RA, Potsdam

In Zusammenarbeit mit/in cooperation with  
DIPL.-CHEM. DR. HANS ULRICH MAY, PA\*, München

PA - Patentanwalt/Patent Attorney  
RA - Rechtsanwalt/Attorney at Law  
\* - European Patent Attorney  
+ - Brandenburg, zugelassen am OLG Brandenburg  
o - Maître en Droit  
Alle zugelassen zur Vertretung vor dem Europäischen Markenamt, Alicante  
Professional Representatives at the Community Trademark Office, Alicante

Ihr Zeichen  
Your ref.

Ihr Schreiben  
Your letter of

Unser Zeichen  
Our ref.

Bremen,

Neuanmeldung  
Gebrauchsmuster

A10026

27. September 2000

Andersen Consulting Unternehmensberatung GmbH, Otto-Vogler-Straße 15, 65843 Sulzbach  
"Informationsdienstsystem"

Die vorliegende Erfindung betrifft ein Informationsdienstsystem, insbesondere für die Polizei.

Trotz insgesamt hervorragender Voraussetzungen sieht sich die Polizei in Deutschland – wie auch in anderen Staaten – aktuellen Herausforderungen ausgesetzt, denen zu begegnen mit herkömmlichen Mitteln oft zunehmend schwerer wird.

Diese Herausforderungen umfassen

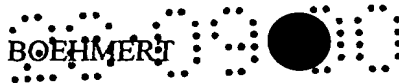
- interne Faktoren, wie Umstrukturierungen innerhalb der Polizeiorganisationen und einen wachsenden Kostendruck, und

- 28.73 -

Hollerallee 32 • D-28209 Bremen • P.O.B. 10 71 27 • D-28071 Bremen • Telephone +49-421-34090 • Telefax +49-421-3491768

MÜNCHEN - BREMEN - BERLIN - DÜSSELDORF - FRANKFURT - BIELEFELD - POTSDAM - BRANDENBURG - KIEL - PADERBORN - HÖHENKIRCHEN - ALICANTE

<http://www.boehmert.de> e-mail: [postmaster@boehmert.de](mailto:postmaster@boehmert.de)



- externe Faktoren, wie eine Zunahme komplexer Kriminalitätsformen, z. B. Wirtschaftskriminalität oder organisierte Kriminalität, und größer werdende Polizeigeographische Räume (Deutschland, Europa) und eine damit verbundene Zunahme grenzüberschreitender Kriminalität.

Derartigen Herausforderungen kann nur durch eine entsprechende Befähigung der Polizei begegnet werden. Der dafür unter anderem erforderliche Zugang zu relevanten Informationen besteht bisher jedoch nur in Fragmenten, das heißt die Polizeiorganisationen der 16 Bundesländer, des Bundeskriminalamtes, des Bundesgrenzschutzes und der Zollverwaltung, die zum Teil ebenfalls Polizeiaufgaben wahrnimmt, können im Prinzip derzeit nicht auf Informationen in einem zur Bearbeitung eines Auftrages ausreichenden Umfang zugreifen.

Der Erfindung liegt somit die Aufgabe zugrunde, ein Informationsdienstsystem zur Verfügung zu stellen, das es einem Benutzer ermöglicht, unabhängig vom zur Verfügung stehenden Zugangskanal (Zugangsweg) auf einfache Weise auf die von ihm benötigten Instrumente, wie Informationen und Applikationen, zuzugreifen.

Erfindungsgemäß wird diese Aufgabe gelöst durch ein Informationsdienstsystem mit Applikationseinrichtungen, insbesondere für die Polizei, mit Informationssystemen, einem intelligenten, dynamisch realisierten Portal für einen einheitlichen Zugang zu den nachgelagerten Informationssystemen mit einem vom Benutzer abhängigen Umfang, mindestens einem Endgerät für einen Zugang zu dem Portal, und mindestens einer Kommunikationseinrichtung zum Verbinden des Endgeräts mit dem Portal. Mit einem intelligenten Portal ist ein Portal gemeint, das auch eigene Funktionen zur Verfügung stellt. Unter einem dynamisch realisierten Portal ist ein Portal zu verstehen, das abhängig vom Kontext (z. B. Datum, Tageszeit, besondere Vorkommnisse, angemeldeter Benutzer etc.) generiert wird. Das Gegenstück dazu stellt ein statisches Portal dar, das zwar regelmäßig mit neuen Informationen „gefüllt“ wird, bei dem aber sonst keine flexible, kontextabhängige Darstellung erfolgt.

DE 200 16 748 U1

Weiterhin kann dabei vorgesehen sein, daß die Informationssysteme mindestens eine externe und/oder mindestens eine lokale Datenbank umfassen. Dabei kann es sich beispielsweise um Datenbanken privater oder öffentlicher Organisationen handeln.

Günstigerweise umfassen die Informationssysteme mindestens eine lokale Media-Datenbank.

Außerdem kann vorgesehen sein, daß die Informationssysteme mindestens ein lokales Data Warehouse umfassen. Ein Data Warehouse ist ein Datenlager beispielsweise für Bild- oder Videodaten.

Günstigerweise umfassen die Informationssysteme mindestens eine lokale Einrichtung für eine Applikation. Beispielsweise kann die Applikation zur Einsatzplanung dienen.

Gemäß einer weiteren besonderen Ausführungsform kann vorgesehen sein, daß die Informationssysteme mindestens ein lokales Bürokommunikationssystem umfassen. Beispielsweise kann das Bürokommunikationssystem zur Erfassung, Bearbeitung, Absendung und Verwaltung von Dokumenten sowie zum Empfangen, Erstellen, Absenden und Dokumentieren von E-mails dienen.

Außerdem kann vorgesehen sein, daß das Portal einen Server umfaßt.

Günstigerweise umfaßt das Portal eine Engine-Schicht mit mindestens einer Engine auf einer Schicht mit einer Administrationseinrichtung zur Verwaltung von Benutzern, Konfiguration der Engine(s) und Administration von vor- und nachgelagerten Schichten. Die Engines sind Maschinen zur Erfüllung gewisser Aufgaben des Portals.

Vorzugsweise umfaßt das Portal in einer vorgelagerten Schicht eine Einrichtung zur Authentifizierung eines Benutzers und des Servers. Es handelt sich dabei um eine Hardware-Schicht, die dazu dient zu klären, wer mit wem kommuniziert.

DE 200 18 748 U1

Außerdem umfaßt die Einrichtung zur Authentifizierung günstigerweise eine Einrichtung zur Identifizierung eines Benutzers.

Vorteilhafterweise umfaßt das Portal in der vorgelagerten Schicht eine Authorisierungssteuer- und eine -speichereinrichtung zur Regelung des Umfangs des Zugangs eines Benutzers. Die Authorisierungssteuerung kann dabei über Benutzer- und Benutzergruppenrechte erfolgen.

Günstigerweise weist das Portal eine Einrichtung zur Darstellung der Nutzungsmöglichkeiten des Portals in Abhängigkeit vom äußeren Kontext, wie z. B. Datum, Tageszeit, Benutzer, besondere Vorkommnisse, auf.

Gemäß einer weiteren besonderen Ausführungsform der Erfindung kann vorgesehen sein, daß das Portal in der vorgelagerten Schicht eine Einrichtung zur Verschlüsselung der über die Kommunikationseinrichtung gesendeten Daten und zur Entschlüsselung der über die Kommunikationseinrichtung empfangenen Daten umfaßt. Eine derartige Einrichtung dient zum Schutz der über das Informationsdienstsystem abfragbaren sensitiven Daten vor unberechtigtem Abhören.

Weiterhin umfaßt das Portal vorteilhafterweise eine Einrichtung zur Wahrung bzw. Feststellung der Integrität der über die Kommunikationseinrichtung gesendeten und empfangenen Daten. Damit soll eine unzulässige Manipulation der übertragenen Daten verhindert bzw. nachgewiesen werden.

Entsprechend einer weiteren besonderen Ausführungsform der Erfindung kann vorgesehen sein, daß die Engine-Schicht eine Abonnement-Engine zum Abonnieren von Informationen, Verzeichnissen und weiteren Diensten durch einen Benutzer umfaßt. Damit kann ein Benutzer dem Informationsdienstsystem seine Interessen mitteilen (aktive Personalisierung) und bekommt er Neuigkeiten in diesen Interessengebieten z. B. nach dem Einloggen mitgeteilt.

DE 200 15 746 U1

Vorteilhafterweise umfaßt die Engine-Schicht eine Filter-Engine. Die Filter-Engine kann die für den jeweiligen Benutzer unterschiedlichen Informationsbereiche nach vorgegebenen Kriterien untersuchen. Das heißt, sobald ein Benutzer eine Personen-, Sach- oder andere Art von Abfrage vornimmt, greift die Filter-Engine auf ihr bekannte Informationsquellen zu und stellt sie eine Liste aus allen Suchergebnissen zusammen.

Außerdem kann vorgesehen sein, daß die Engine-Schicht eine Information Repository-Engine und/oder eine Application Repository-Engine und/oder Office communication Repository-Engine umfaßt. Die Information Repository-Engine kann eine Metadatenstruktur der nachgelagerten Informationssysteme und Pfadinformationen für einen Zugriff auf dieselben beinhalten. Die Information Repository-Engine wird von Diensten genutzt, für die nicht der Speicherort, aber der Typ der Informationen (Sache, Person, ...) relevant ist. So sind beispielhaft Personeninformationen in verschiedenen Informationssystemen gespeichert: LKA, BKA und Interpol. Anstatt allen Diensten die Information zu geben, welche Informationssysteme Personenauskünfte beinhalten, reicht es im Dienst, anhand der Anfrage „Personen“ alle notwendigen Speicherorte über die Information Repository-Engine zu ermitteln. Eine Application Repository-Engine beinhaltet ein Verzeichnis über die Applikationen, die den Benutzern des Informationsdienstsystems über das Portal in den nachgelagerten Informationssystemen zur Verfügung stehen. Sie beinhaltet neben dem Ort der Applikation auch eine Information über die für den Zugriff notwendigen Benutzer- und Benutzergruppenrechte. Erfolgt beispielhaft der Zugriff auf INPOL durch einen PVB (Polizeivollzugsbeamter), dann ist dieser Zugriff aufgrund seiner Benutzergruppenzugehörigkeit zulässig und wird die Verbindung zu INPOL aufgebaut. Wenn hingegen ein VB (Verwaltungsbeamter) auf INPOL zugreifen möchte, wird der Zugang verweigert, da der VB aufgrund seiner Benutzergruppenzugehörigkeit keine Berechtigung besitzt. Im Falle einer erweiterten Befugnis kann dem VB die INPOL-Berechtigung auf Benutzerebene zugeteilt und der Zugriff auf INPOL wiederum ermöglicht werden. Die Office communication Repository-Engine bietet einen einheitlichen Zugang zu einem lokalen Bürokommunikationssystem und dessen angegliederten Funktionalitäten.

DE 200 16 746 U1

Günstigerweise umfaßt das Portal eine Output-Engine. Mittels der Output-Engine wird einem Benutzer die Möglichkeit gegeben, Informationsobjekte über unterschiedliche Zugangskanäle in verschiedenen Formaten zu erhalten.

Günstigerweise umfaßt das Portal einen Schnittstellen-Integrator für die nachgelagerten Informationssysteme. Durch das Portal müssen nämlich unterschiedliche Schnittstellen unterstützt werden, da in großen Organisationen, wie z. B. der Polizeiorganisation, der Zugriff auf verschiedenste Informationssysteme notwendig ist. Dazu zählen neben den verschiedenen Plattformen und Systemarchitekturen auch differierende Informationsquellen, Datendarstellungen und unterschiedliche Datenbanken, wie relationale und multidimensionale Datenbanken sowie unstrukturierte Datenspeicher. Weiterhin werden dadurch auch Schnittstellen zu Data Warehouse und Data Mining Systemen realisiert.

Vorzugsweise umfaßt das Portal mindestens ein Mehrwertdienstsystem. Das Mehrwertdienstsystem bietet einen spezifischen Dienst und ist ein Teil des Portals und gehört damit nicht einem nachgelagerten Informationssystem an. Jedes Mehrwertdienstsystem kontrolliert die Zugangsberechtigung selbst, das heißt bei Aufruf eines solchen Mehrwertdienstsystems überprüft dieses anhand des Benutzerprofils und der für den Mehrwertdienst notwendigen Berechtigungen, ob die Benutzer- oder Benutzergruppenrechte für eine Nutzung des Mehrwertdienstes ausreichend sind. Bei nicht ausreichender Berechtigung wird der Zugriff auf den Mehrwertdienst verweigert.

Außerdem enthält das Portal günstigerweise einen Request Broker. Dieser ordnet anhand der Art der Benutzeranfrage diese der richtigen Engine zu und sorgt nach Abarbeitung der Anfrage dafür, daß die gewonnenen Informationen an den korrekten Benutzer zurückübermittelt werden.

Eine weitere besondere Ausführungsform der Erfindung ist gekennzeichnet durch eine Firewall machine zwischen dem Portal und der mindestens einen Kommunikationseinrichtung.

DE 200 18 746 U1

Diese dient zur Realisierung einer Firewall und überwacht den gesamten Datenverkehr zwischen den Endgeräten und dem Portal, um unbefugtes Eindringen in das Informationssystem, Einbringen von Virus-Programmen und ähnliche Attacken abzuwehren.

Schließlich ist eine weitere besondere Ausführungsform der Erfindung gekennzeichnet durch eine Firewall machine zwischen dem Portal und den nachgelagerten Informationssystemen. Diese hat dieselbe Funktion wie die vorgenannte Firewall machine, aber hinsichtlich des Übergangs Portal-nachgelagerte Informationssysteme.

Der Erfindung liegt die überraschende Erkenntnis zugrunde, daß über einen einheitlichen Zugang, nämlich das Portal, die verfügbaren Daten und Applikationseinrichtungen der unterschiedlichsten Organisationen auf leichte Weise zugänglich gemacht werden, wodurch jeder beispielsweise Polizeibeamte unabhängig vom Zugangskanal funktionsbezogene Informationen erhalten kann und somit befähigt wird, seinen Auftrag abzuarbeiten. Darüber hinaus ermöglicht das Portal die Verknüpfung der zugänglich gewordenen Informationen und Applikationseinrichtungen, wodurch diese damit indirekter Bestandteil des Portals werden. Durch Herstellung des Zusammenhangs aus den Daten der vorhandenen Informationssysteme und Applikationseinrichtungen läßt sich eine neue Qualität der Information schaffen und damit ein für beispielsweise die Polizei notwendiger Mehrwert erzeugen. Die notwendigen Informationen werden in ihrem Kontext dargestellt, wodurch die Polizei besser zur Wahrnehmung ihrer Aufgaben befähigt wird und strategische Ziele konsequenter verfolgt werden können.

Darüber hinaus ermöglicht die Verwendung eines Portals neben der Integration bestehender Informationssysteme und Applikationseinrichtungen auch die Identifikation, Realisierung und Integration von zukünftigen Informationssystemen und Applikationseinrichtungen. Neue Informationssysteme und Applikationseinrichtungen können nach ihrer Erstellung auf Basis der Architektur des vorliegenden Informationssystems auf einfache und einheitliche Weise zur Verfügung gestellt und mit bestehenden Informationssystemen verknüpft werden. Die Polizei kann damit in denjenigen Bereichen unterstützt werden, in denen durch mangelnde



Instrumente die vorhandenen Potentiale gegenwärtig nicht vollständig ausgeschöpft werden. Beispielsweise könnten ein operatives Controlling, Instrumente des Risikomanagements oder Trainings- und Wissensapplikationen integriert werden.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus den Ansprüchen und der nachfolgenden Beschreibung, in der ein Ausführungsbeispiel anhand von Zeichnungen erläutert ist. Dabei zeigt:

Figur 1 schematisch die technische Architektur einer besonderen Ausführungsform eines Informationsdienstsystems gemäß der vorliegenden Erfindung;

Figur 2 schematisch durch unterschiedliche Zugangsberechtigungen resultierende Sicherheitszonen;

Figur 3 schematisch die funktionale Systematik der besonderen Ausführungsform des Informationsdienstsystems von Figur 1; und

Figur 4 schematisch ein Anwendungsbeispiel.

Figur 1 zeigt schematisch die technische Architektur einer besonderen Ausführungsform eines Informationsdienstsystems gemäß der vorliegenden Erfindung. Das Informationsdienstsystem läßt sich grob in drei Komponenten unterteilen: A: Zugangskanäle; B: Intelligentes Portal und C: Nachgelagerte Informationssysteme. Die Zugangskanäle dienen zur Herstellung eines Zugangs zu einem intelligenten, dynamisch realisierten Portal und werden durch jeweilige Endgeräte 10 bis 16 und Kommunikationseinrichtungen realisiert. Hinsichtlich des Zugangs wird zwischen einem

- lokalen Zugang

DE 200 16 748 U1

- ortsunabhängigen Zugang mittels eines mobilen PC's
- ortsunabhängigen Zugang mit datenfähigen Endgeräten und
- ortsunabhängigen Zugang mit nicht-datenfähigen Endgeräten

unterschieden. Dabei kann jeder autorisierte Benutzer jeden beliebigen Zugangskanal im Wechsel nutzen.

Bei einem lokalen Zugang besitzen Benutzer feste, an einen Platz gebundene Arbeitsplätze, wie dies durch das Endgerät 10 in Form eines PC dargestellt werden soll. Die Kommunikationseinrichtung zum Verbinden des Endgeräts mit dem Portal B umfaßt eine Datenfernübertragungseinrichtung 18 in Form eines Telefonfest- bzw. Mobilfunknetzes, einen Router 20 (Knotenrechner zwischen Datennetzen) und das Internet, wobei bezüglich letzterem Web-Browser auf HTML-Basis und als Netzwerkprodukt einheitliche TCP/IP-Netze eingesetzt werden. Ein HTTP-Server 22 steht in Figur 1 stellvertretend für das Internet. Dies erlaubt einen durchgehenden und einheitlichen Einsatz von Bürokommunikationssystemen.

Einen ortsunabhängigen Zugang mit mobilen PC's besitzen vollwertige, jedoch nicht an einem Platz gebundene Arbeitsplätze, wie das in Figur 1 gezeigte Endgerät 12 in Form eines Laptops bzw. Notebooks. Die Kommunikationseinrichtung zum Verbinden des Endgeräts 12 mit dem Portal B sieht genauso aus wie bei dem Endgerät 10. Gegenüber einem an einem festen Platz befindlichen PC (siehe Endgerät 10) weist ein Endgerät 12 die Möglichkeit auf, daß sich ein Benutzer mittels in dem Laptop bzw. Notebook eingebundenen Kommunikationsmechanismen von unterschiedlichen Orten aus in das Portal B einwählen kann und dann die gleichen Funktionen wie bei Verwendung eines stationären PC's zur Verfügung gestellt erhält.

DE 200 16 746 U1

Bei einem ortsunabhängigen Zugang mit datenfähigen Endgeräten, wie z. B. dem mit dem Bezugszeichen 14 gekennzeichneten Endgerät, umfaßt eine zugehörige Kommunikationseinrichtung eine Datenfernübertragungseinrichtung 18 in Form eines Mobilfunknetzes, einen Router 20 sowie einen WAP (Wireless Application Protocol)-Server 24 mit einem WAP-Browser auf WML-Basis. Als Netzwerkprodukt kommen einheitliche TCP/IP-Netze zum Einsatz.

Schließlich stellen klassische Mobilfunktelefone ein Beispiel für nicht-datenfähige Endgeräte 16 dar, die einen ortsunabhängigen Zugang ermöglichen. Die zugehörige Kommunikationseinrichtung für ein klassisches Mobilfunktelefon umfaßt eine Datenfernübertragungseinrichtung 26 in Form eines Mobilfunknetzes und einen IVR-(Interactive Voice Response)-Server 28, also ein interaktives Sprachsystem, das es einem Benutzer ermöglicht, selektiv Informationen abzufragen wie auch gezielt Informationen zu erhalten. Sofern das Endgerät 16 bereits WAP-fähig sein sollte, können die Informationen auch über den WAP-Server 24 auf WML-Basis abgefragt und erhalten werden.

Zwischen den Zugangskanälen A und dem Portal B sowie dem Portal B und den nachgelagerten Informationssystemen C ist jeweils eine Fire Wall Machine 30 bzw. 32 angeordnet. Das Portal B umfaßt einen Applikations-Server 34. Die nachgelagerten Informationssysteme C umfassen unter anderem eine externe Datenbank 36, beispielsweise INPOL, die über einen Router 38 und ein WAN-(Wide Area Network) 40 zugänglich ist, eine lokale Einrichtung 42 für eine Applikation, beispielsweise Einsatzplanung, ein lokales Bürokommunikationssystem 44, ein lokales Data Warehouse 46 und einen Drucker 48.

Aufgrund der Sensitivität der mittels des Informationsdienstsystemes verfügbaren Daten ist der Sicherheitsaspekt von wesentlicher Bedeutung. Dabei setzt sich der Begriff der Sicherheit im Kontext von netzwerkbasierten Applikationen aus folgenden Elementen zusammen:

- a) Server- und Client-seitige Authentifizierung – Wer kommuniziert mit wem?

- b) Authorisierung – Welche Zugriffsberechtigung hat der anfragende Benutzer?
- c) Datensicherheit – Kann die Datenübertragung abgehört werden?
- d) Datenintegrität – Kommen die Daten bei der Übertragung so an, wie sie gesendet wurden?

Nicht jeder Benutzer gelangt ohne weiteres an alle über das Portal zur Verfügung stehenden Daten. Der Zugang zu den Informationen ist nämlich grundsätzlich in drei verschiedene Sicherheitszonen (siehe Figur 2) unterteilt:

- Internet

In diese Zone können alle nicht definierten Benutzer ohne Berechtigung auf sensitive Daten, die einen Gaststatus aufweisen, gelangen. Der Zugriff ist nur auf statische Seiten möglich, die allgemeine Informationen über das Informationssystem bereitstellen. Die einzige Kontaktmöglichkeit in dieser Sicherheitszone besteht in einer E-mail an den Betreiber des Portals B. Eine Personalisierung der Inhalte ist nicht möglich.

- Extranet

Alle glaubwürdigen („trusted“) Benutzer 50, 52 des Informationssystemes haben die Möglichkeit, nach einer Authentifizierung Inhalte einzustellen. Nur ein Teil der Benutzer, nämlich die Benutzer 52, hat auch die Möglichkeit, Abfragen von Inhalten vorzunehmen. Zu den Benutzern, die in das Extranet gelangen, gehören alle privatrechtlichen Organisationen oder Organisationen des öffentlichen Rechts, die nicht der Polizei angehören.

7. Aufforderung zur Identifizierung des Clients über symmetrische Verschlüsselung (Sessionkey)
8. Identifizierung des Benutzers in Abhängigkeit von der Sicherheitszone, wobei keine Identifizierung notwendig ist, wenn ein Benutzer der Sicherheitszone (Internet) angehört, während ein Identifikationsverfahren notwendig ist, wenn ein Benutzer den Sicherheitszonen „Extranet“ oder „Intranet“ angehört. Bei einem Gastzugang ist keine Identifikation erforderlich, während bei einem Extranetzzugang eine Identifikation über Benutzernamen und Passwort vonstatten gehen kann und bei einem Intranetzzugang die Identifikation in Form eines Benutzernamens/Chipcard in Verbindung mit einem biometrischen Verfahren (Fingerabdruck, Sprecheranalyse, Irisanalyse) erfolgen kann.
9. Gewährung des Zugangs nach Identifikation im Applikations-Server 34.

Bei einem Zugang über nicht-datenfähige Endgeräte (Sprechverbindungen) kann die Server- und Client-seitige Authentifizierung wie folgt ablaufen:

1. Einwahl über eine dezidierte Zugangsnummer des Informationsdienstsystemes
2. Eingabe der Benutzerkennung über eine Telefontastatur, wobei ein MFW-fähiges Telefon vorausgesetzt wird
3. Zusätzliche Identifizierung über Sprechererkennung
4. Registrierung der Anrufernummer

- Intranet

In diese Sicherheitszone gelangen alle polizeiinternen Benutzer. Nach einer Authentifizierung erfolgt ein personalisierter Aufbau des Portals B. In dieser Sicherheitszone erfolgt der lesende und schreibende Zugriff auf alle für den Benutzer zugelassenen Informationssysteme. Zur Erzielung eines hohen Sicherheitsstandards kann die oben unter a) genannte Server- und Client-seitige Authentifizierung wie folgt ablaufen:

- Zugang über datenfähige Endgeräte

Zur Sicherstellung, daß der gewünschte Applikations-Server 34 von einem berechtigten Client (Benutzer) erreicht wird, kann wie folgt vorgegangen werden:

1. Anfrage über den HTTP-Server 22 oder WAP-Server 24
2. Rückmeldung des Portals B mit Zertifikat, öffentlichem Schlüssel (asymmetrisches Verschlüsselungsverfahren) und Signatur
3. Client-seitige Erzeugung eines Sessionkeys für die aktuelle Verbindung
4. Verschlüsselung des Sessionkeys mit öffentlichem Schlüssel von Portal B
5. Versand an Applikations-Server 34
6. Entschlüsselung des Sessionkeys mit privatem Schlüssel des Informationssystems

Die oben unter b) angesprochene Authorisierung kann innerhalb des Portals B auf Applikationsebene erfolgen; das heißt je Benutzer liegt ein Profil vor, das ihm erlaubt, auf bestimmte Funktionen zuzugreifen. Dabei wird die Authorisierung im Gegensatz zur optimistischen Steuerung, bei der dem Benutzer Zugriffsrechte „weggenommen“ werden und er von Anfang an alle Möglichkeiten hat, pessimistisch gesteuert. Ein Benutzer muß Zugriffsrechte explizit zugeordnet bekommen.

Die Authorisierungssteuerung erfolgt über Benutzer- und Benutzergruppenrechte. Hierbei ist jeder Benutzer zumindest einer Benutzergruppe zugeordnet. Die Benutzerrechte haben gegenüber den Benutzergruppenrechten eine höhere Priorität. Ist beispielhaft ein Benutzer gemäß einer Benutzergruppenzugehörigkeit nicht berechtigt, eine bestimmte Applikation zu nutzen, kann er aufgrund erweiterter Befugnisse diese Berechtigung persönlich zugeordnet bekommen. In diesem Fall gilt die Berechtigung auf Benutzerebene.

Die Authorisierungsspeicherung erfolgt in Abhängigkeit von der Sicherheitszone:

- Internet

Der Benutzer hat nur Gastzugang und kann keine Applikationen aufrufen. Die Speicherung der Zugriffsrechte erfolgt in einer Datenbank als Profil „Gast“ der Benutzergruppe „Gäste“.

- Extranet

Der Benutzer hat einen personalisierten Zugang, das heißt er muß sich im Informationssystem anmelden. Der Zugriff auf polizeiliche Applikationen wird verweigert. Applikationen zum Content Management sind zulässig. Die Speicherung erfolgt in einer Datenbank per Benutzernamen und zu einer spezifischen Benutzergruppe, wie z. B. „Verkehrsbetriebe“, „Diplomaten“, etc...

DE 200 15 746 U1

- Intranet

Der Benutzer hat einen personalisierten Zugang und hat in der Regel die Rolle eines PVB (Polizeivollstreckungsbeamter) oder VB (Verwaltungsbeamter). Der Zugriff auf polizeiliche und andere Applikationen ist teilweise bis voll erlaubt. Die Speicherung erfolgt in der Datenbank per Benutzernamen und zu einer oder mehreren spezifischen Benutzergruppen, wie z. B. „PVB“, „Dienststellenleiter“, „SoKo“, etc. Da dieser Benutzerkreis in der Regel auch Zugriff auf das Dateisystem direkt hat (Bürokommunikation etc.), ist ein Profil noch mit dem jeweiligen Benutzerprofil des Betriebssystems verbunden (NT, LDAP, etc.).

Die oben unter c) genannte Datensicherheit wird mittels eines Verschlüsselungsmechanismus hergestellt, der alle über eine aktive Sitzung gesendeten und empfangenen Daten verschlüsselt und entschlüsselt. Dabei beginnt eine Sitzung mit dem Einloggen des Benutzers. Sie ist beendet, sobald sich ein Benutzer abgemeldet hat oder für eine definierte Zeit, z. B. 30 Minuten, nicht mehr aktiv war. Die Verschlüsselung erfolgt über ein symmetrisches Verfahren. Hierzu benötigen beide Seiten einen identischen Schlüssel. Dieser wird wie oben zu a) beschrieben erstellt und hat nur Gültigkeit für eine Sitzung.

Im Zusammenhang mit der oben unter d) genannten Datenintegrität ist zwischen dem Transfer von HTML/WML-Daten und von E-mails zu unterscheiden. Im erstgenannten Fall erfolgt eine Datenintegritätssicherung durch die Verschlüsselung der übertragenen Daten mit einem eigenen symmetrischen Schlüssel je Sitzung. Im letztgenannten Fall erfolgt die Sicherung zweistufig. Zum einen werden die übertragenen Daten wie im erstgenannten Fall verschlüsselt. Zum anderen erhält jede E-mail eine Signatur des Absenders.

Nachfolgend soll unter Bezugnahme auf Figur 3 auf die funktionale Systematik des intelligenten, dynamisch realisierten Portals B näher eingegangen werden. Es handelt sich dabei um ein dynamisches Portal, da die Inhalte des Portals in Abhängigkeit vom äußeren Kontext dargestellt werden. Der äußere Kontext setzt sich dabei aus folgenden Elementen zusammen:

DE 200 16 746 U1



- Datum, Uhrzeit
- Benutzer
- besondere polizeirelevante Ereignisse.

Das Portal B übernimmt die Funktion eines Mittlers der Benutzer, die über einen der oben beschriebenen Zugangskanäle an das Portal B angebunden sind, und den nachgelagerten Informationssystemen der Polizei. Dem intelligenten Portal B fallen dabei unterschiedliche Aufgaben zu, die mittels unterschiedlicher sogenannter Engine(s) realisiert werden. Damit den Benutzern von diesen Engine(s) die gewünschten, für sie wichtigen und notwendigen Daten zur Verfügung gestellt werden, erfolgt in einer vorgelagerten Schicht in einer Einrichtung 54 zur Authentifizierung und Identifizierung eines Benutzers eine Authentifizierung bzw. Personalisierung. Dahinter sind in einer Engine-Schicht eine Abonnement-Engine 56, eine Filter-Engine 58, eine Information Repository-Engine 60, eine Application Repository-Engine 62 und eine Office Communication Repository-Engine 64 angeordnet, deren Aufgaben bereits oben erläutert worden sind. Die Filter-Engine und die Abonnement-Engine stellen dabei intelligente Agenten dar. Die Engine(s) selbst kommunizieren zur Abdeckung ihrer Aufgaben Engine-Informationsbereiche über fest spezifizierte Schnittstellen mit den im Hintergrund arbeitenden unterschiedlichen Systemen der Informationsverarbeitung.

Die Engine-Schicht befindet sich auf einer Schicht mit einer Administrationseinrichtung (nicht gezeigt) zur Verwaltung von Benutzern, Konfiguration der Engine(s) und Administration von vor- und nachgelagerten Schichten.

Die nachgelagerten Systeme C umfassen zwei externe Datenbanken 36a, 36b einer privaten und einer öffentlichen Organisation, eine lokale Einrichtung 42 für eine Applikation, ein lokales Bürokommunikationssystem 44, ein lokales Data Warehouse 46, eine lokale Mediadatenbank 43 und lokale Datenbanken 45.

DE 200 18 748 U1

Die in Figur 3 gezeigten Komponenten decken die verschiedenen Gebiete der Aufgabenstellung der Polizei vollständig ab. Der Zugang zu den einzelnen Applikationen und Mehrwertdiensten, von denen einer dargestellt und mit dem Bezugszeichen 66 versehen ist, durch das Portal B wird durch die Zuordnung von Benutzer- und Benutzergruppenrechten gesteuert. Damit werden jedem Beamten genau diejenigen Applikationen zur Verfügung gestellt, die er für die Wahrnehmung seiner spezifischen Aufgaben benötigt. Durch die Integration der vorgenannten Komponenten in dem Informationsdienstsystem werden sie in ihrem Sinnzusammenhang dargestellt. Hierdurch wird die Verknüpfung der vorhandenen Daten zu Informationen erleichtert.

Eine Request Broker 68 ordnet anhand der Anfrage diese der richtigen Engine zu und sorgt nach der Abarbeitung der Anfrage dafür, daß die gewonnenen Informationen an den korrekten Benutzer zurück übermittelt werden. Über eine Output-Engine 70 wird dem Benutzer die Möglichkeit anhand gegeben, Informationsobjekte über unterschiedliche Kommunikationskanäle in verschiedenen Formaten zu erhalten. Außerdem ist ein Schnittstellen-Integrator 67 vorgesehen.

Das Portal B ermöglicht die Umsetzung der Idee der operativen Arbeit der Polizei. Über einen einheitlichen Zugang, das Portal, werden die verschiedenen Applikationseinrichtungen (Legacy Systeme) der Polizei zugänglich gemacht und miteinander verknüpft und werden damit indirekter Bestandteil des Portals. Wichtig ist dabei die Herstellung des Zusammenhangs aus den Daten der vorhandenen Applikationseinrichtungen, um eine neue Qualität der Information zu schaffen und damit den für die Polizei notwendigen Mehrdienst zu generieren. Die notwendigen Informationen werden in ihrem Kontext dargestellt, wodurch die Polizei besser zur Wahrnehmung ihrer Aufgaben befähigt wird und strategische Ziele konsequenter verfolgt werden können.

DE 200 18 748 U1

Neben der Integration bestehender Applikationseinrichtungen auf der Basis der obigen beschriebenen Architektur des Portals beinhaltet die Erfindung auch die Identifikation, Realisierung und Integration von zukünftigen Applikationseinrichtungen in das Portal.

Neue Applikationseinrichtungen können nach ihrer Erstellung auf Basis der hier beschriebenen Architektur auf einfache und einheitliche Weise zur Verfügung gestellt und mit bestehenden Informationssystemen verknüpft werden. Die Polizei kann damit in denjenigen Bereichen unterstützt werden, in denen durch mangelnde Instrumente die vorhandenen Potentiale gegenwärtig nicht vollständig ausgeschöpft werden. Beispielsweise könnten ein integratives Controlling, Instrumente des Risikomanagements oder Trainings- und Wissensapplikationseinrichtungen integriert werden.

Durch den integrativen Aspekt des Portals werden Informationen aus den unterschiedlichen Applikationen miteinander verknüpft und den Benutzern bedarfsgerecht zur Verfügung gestellt. Aus aktuellen Falldaten und archivierten Informationen über vergangene Fälle können z. B. Einsatzempfehlungen und Handlungsalternativen abgeleitet werden. Ein anderes Beispiel wäre eine Nachrichtenseite, die geographisch regionalisiert und auf Benutzergruppen bezogen angezeigt wird. Auf diese Weise wird ein Beamter mit aktuellen, regionalen, polizei-relevanten Ereignissen vertraut gemacht. Beispielsweise erhält er Fahndungsmeldungen oder lokale Ereignisse und Aktivitäten. Diese sogenannten Mehrwertdienste schaffen durch die intelligente Verknüpfung und Darstellung von gegebenen Datenwerten in Form von aggregierten und selektierten Informationen für die Polizei.

Das visuelle Kernstück des Informationsdienstsystems kann aus einer Startseite bestehen, die Links zu den integrierten Applikationen und Mehrwertdiensten enthält. Die Links sind gruppiert in integrierte Applikationen, Mehrwertdienste und persönliche Applikationen. Die persönlichen Applikationen umfassen z. B. E-mail, Einsatzplanung und lokale Ereignisse, aber auch persönliche Suchagenten, rekrutieren sich also sowohl aus den integrierten Applikatio-

DE 200 16 746 U1

- (b) Externes Ergebnis, z. B. Aufklärungsquote, subjektives Sicherheitsempfinden, Häufigkeitszahlen
- (c) Prozesse, z. B. Verhältnis von wertschöpfenden zu administrativen Tätigkeiten, durchschnittliche Aufklärungszeit, Verhältnis von Festnahmen zu Verurteilungen
- (d) Organisation, z. B. Krankheitsrate, wahrgenommene Fortbildungsprogramme, Zahl umgesetzter Verbesserungen.

Die Neuerung besteht in der Verfügbarkeit und Erreichbarkeit von Informationen. Aktuell werden diese Informationen händisch ermittelt und dann in Form von E-mail an die betreffenden und andere Personen gesendet. Die Integration über das Portal des Informationsdienstsystems bedeutet, daß die relevanten Informationen den betroffenen Personen über das Portal mittels Abonnements oder Suche bereitgestellt werden.

#### Befähigung

Der Anwendungsfall „Befähigung“ bezieht sich auf Ausbildungsmaßnahmen, die über das Portal angeboten werden können. Durch die eingesetzte Technologie wird es dem Beamten ermöglicht, in seiner Arbeitsumgebung (beispielsweise Dienststelle) Online, bedarfsgesteuert Schulungsangebote wahrzunehmen. Diese Schulungsangebote umfassen interaktive Lernprogramme, die angefangen bei elektronischen Nachschlagewerken über einfache, dialoggesteuerte bis mediale Schulungen gehen.

#### Administrative Unterstützung

Die administrative Unterstützung durch das Portal umfaßt sowohl alle mit Fällen verbundenen Aufgaben wie auch alle persönlichen administrative Tätigkeiten. Diese Tätigkeiten sind erforderlich, nehmen allerdings viel Zeit in Anspruch. Durch den Einsatz des Portals findet eine

DE 200 16 746 U1

nen als auch aus den Mehrwertdiensten. Es sind diejenigen Komponenten des Portals, die am häufigsten genutzt werden und daher am leichtesten zugänglich gemacht werden sollen.

Das intelligente Portal verbindet vorhandene oder zukünftige Applikationen der Polizei und schafft durch eine gemeinsame Oberfläche und integrierte Dienste zusätzlichen Wert aus gegebenen Daten. Die einzelnen Komponenten können bestehende Applikationen sein, die auch selbständig existieren könnten, wie etwa E-mail oder operatives Informationssystem, oder zukünftige Applikationen, die dann in das Portal integriert werden.

Zur umfassenden Unterstützung der polizeilichen Aufgaben ist die Integration von Applikationen aus den folgenden Bereichen möglich:

#### Zielorientierte Steuerung

Dieser Anwendungsfall umfaßt alle Auswertungen von operativen Daten, die der detaillierten Einsatzplanung dienen. Dazu gehören (a) Erfassung von Informationen, (b) Verknüpfung von Informationen, (c) geographische Darstellung der Informationen (regionale Auswertung von Tatbeständen) und (d) Bereitstellung von Informationen für Controlling und Risk Management.

#### Operatives Informations- und Steuerungssystem

Dieser Anwendungsfall umfaßt die Bereitstellung von Steuerungsinformationen. Steuerungsinformationen lassen sich in folgende Bereiche unterteilen:

(a) Internes Ergebnis, z. B. Kostenrechnung

DE 200 16 746 U1

Integration von verfügbaren Informations-Ressourcen statt, so daß durch die Bündelung eine Effizienzsteigerung erreicht wird. Beispielhaft ist hier die unmittelbare Informationsbeschaffung am Ort des Geschehens, daraufhin die Erfassung weiterer spezifischer Informationen und anschließend die Administration der Informationen in Form von einzelnen Berichten. Im konkreten Beispiel liegen über das Portal alle notwendigen Informationen unmittelbar zur Verfügung und können an einem anderen Ort ohne vorherige Wiederbeschaffung der Informationen weiterverarbeitet werden. Aktuell werden diese Informationen über Funk und damit über einen zusätzlichen Mitarbeiter abgefragt. Danach werden diese Informationen notiert und um spezifische Informationen erweitert. Diese werden zwischenzeitlich per Funk an einen anderen Beamten (z. B. Einsatzleiter) weitergeleitet und notiert. Nach Hinzukommen von weiteren Informationen werden diese Informationen erfaßt und im ungünstigen Fall die initiale Informationsabfrage wiederholt.

Bei jedem Beamten fallen auch persönliche administrative Tätigkeiten an. Diese lassen sich durch verschiedene in das Portal integrierte Applikationen vereinfachen. Durch Personalisierung von einzelnen für den Beamten relevanten Informationen kann dieser automatisch mit diesen versorgt werden. Der Vorgang der Beschaffung dieser Art von Informationen durch den Beamten selbst entfällt. Beispielhaft kann ein Beamter automatisch mit neuen Schulungsangeboten zu seinem Spezialgebiet versorgt werden.

#### Mehrwertdienste

Bei diesen Diensten handelt es sich um solche, die die Informationsabfrage und die Erfassung von aktuellen Daten ermöglichen. Beispielhaft können aktuelle Lagedaten vor Ort, das heißt in der Dienststelle oder am Ort des Geschehens erfaßt und gesendet werden. Die Aggregation, Kategorisierung und Auswertung der Daten erfolgt automatisiert. Die automatisiert erstellten Auswertungen werden dann in Abhängigkeit von Personalisierungsmechanismen den betreffenden Beamten zugestellt. Dieser Vorgang kann durch die Bereitstellung der Mehrwertdien-

DE 200 16 746 U1

ste „just-in-time“ erfolgen. Der bisherige Prozeß erforderte mehrfach manuelle Tätigkeiten und benötigte 24 Stunden oder mehr.

Nachfolgend soll ein möglicher Anwendungsfall des erfindungsgemäßen Informationsdienstsystems skizziert werden. Der Anwendungsfall betrifft die Integration des Informationsdienstsystems in den Alltag eines Polizeivollzugsbeamten, der mit einem Endgerät in Form eines WAP-fähigen Gerätes ausgestattet ist. Er dient auch zur Verdeutlichung, wie die Integration der Informationssysteme durch das Portal dem Polizeivollzugsbeamten PVB einen Mehrwert bringt, den er ohne das Portal nicht haben kann.

Szenario: POM Peter Sicher trifft zum Dienstbeginn im ersten Revier seiner Heimatgemeinde Schönstadt ein. POM Sicher und sein Kollege PM Zabel fahren mit ihrem Dienstfahrzeug in das ihnen über das Informationsdienstsystem zugeteilte Stadtgebiet.

- (a) POM Sicher schaltet das im Dienstfahrzeug installierte WAP-fähige Gerät ein. Nachdem sie das Zielgebiet erreicht haben, erhalten sie die Information, daß sich der Dienstplan aufgrund des Ausfalls zweier Kollegen ändert und sie in einem anderen Stadtgebiet eingesetzt werden. Da beide über dieses Stadtgebiet nicht informiert sind, rufen sie den Mehrwertdienst „Risikomanagement“ des Informationsdienstsystems auf. Dort erfahren beide, daß es in den letzten Monaten in dem eigentlich ruhigen Wohngebiet vermehrt zu Einbrüchen gekommen ist. Obwohl das Gebiet deutlich eingegrenzt werden konnte, sind bisher keine Tatverdächtigen ermittelt worden. POM Sicher und PM Zabel entscheiden sich, im betreffenden Gebiet mehr Präsenz zu zeigen.
- (b) In seinem persönlichen Abonnement bekommt POM Sicher die Meldung, daß in 4 Wochen eine Schulung verfügbar wird, die sich auf sein Spezialgebiet „Beschaffungskriminalität“ bezieht. Er meldet sich unmittelbar an und erhält die automatische Rückmeldung, daß für ihn ein Platz reserviert wurde. Automatisch werden ihm vorbereitete Unterlagen in sein elektronisches Postfach gesendet und die Schulung im Einsatzplanungssystem vor-

gemerkt. Sein Einsatzleiter PHM Haupt erhält ebenfalls eine elektronische Mitteilung, die dieser sofort in der Dienststelle DS bestätigen kann.

- (c) Bei der Einfahrt in eine Nebenstraße bemerkt PM Zabel, daß ein Fahrzeug unzulässig auf dem Gehweg parkt. Beim Näherkommen merkt er, daß das Fahrzeug nicht abgeschlossen ist. Über das Portal B des Informationsdienstsystems fragt er in der Datenbank 36c INPOL das Kennzeichen des Fahrzeuges ab (siehe Figur 4). Es erscheinen keine Meldungen. Die Filter-Engine (nicht gezeigt) liefert ihm allerdings die Meldung, daß nach dem Fahrzeughalter in der Datenbank 36d EUROPOL gefahndet wird. In der Datenbank 36c INPOL gibt es allerdings noch keine Eintragung. PM Zabel registriert den Standort des Fahrzeugs und leitet die Information an die Dienststelle DS zurück. Über Funkkontakt kontaktiert er den Einsatzleiter, dem inzwischen die erfaßten Informationen, wie auch die EUROPOL-Informationen in seinem Portal B vorliegen.

Der Einsatzleiter veranlaßt alles weitere. POM Sicher und PM Zabel sollen ihr Einsatzfahrzeug in der Nähe parken und erst einmal auf weitere Anweisungen warten.

Am Ende des Tages erhält der Dienststellenleiter DL eine Auswertung aller Vorkommnisse dieses Tages mittels der lokalen Einrichtung 42. Auf Basis dieser Informationen entscheidet der Dienststellenleiter DL über notwendige Anpassungen des Dienstplans für den folgenden Tag. Die Anpassungen am Dienstplan werden gesichert und die betroffenen PVBs über die Änderungen automatisch informiert.

- (d) Wieder in der Dienststelle DS zurück, erstellen POM Sicher und PM Zabel mittels des lokalen Bürokommunikationssystems 44 noch die notwendigen Berichte. Dabei greifen sie auf die im Laufe des Tages gemachten Eintragungen zurück. Da sich bei den meisten Fällen um Standardverfahren handelt, ist der Großteil der Arbeit bereits erledigt. Die bereits vor Ort geschlüsselten Fälle liegen ausgedruckt in ihren Ablagefächern.

DE 200 18 748 U1



Der oben beschriebene Anwendungsfall beschreibt vier Applikationsfälle des Informationssystemes. Jeder Applikationsfall zeigt eine spezifische Funktion, die im aktuellen Polizeidienst nicht oder nur eingeschränkt verfügbar ist:

- (a) Unmittelbare Information über eine Datenauswertung
- (b) Unmittelbare Information über persönliche Interessen/Anliegen
- (c) Intelligente Integration verschiedener Systeme und Bündelung der Informationen zur weiteren Bearbeitung und
- (d) Weiterverwendung mobil erfaßter Daten zur effizienten Bearbeitung von Standardprozeduren.

Figur 4 zeigt die Informationsflüsse zwischen einem Benutzer, nämlich POM Sicher, und Komponenten eines Informationssystemes entsprechend dem vorangehend beschriebenen Anwendungsfall. Dabei kommt den Bezugszeichen folgende Bedeutung zu:

101 Authentifizierung

102a Personalisierung

102b Darstellung des Portals

103 Suchabfrage Kennzeichen

104a Search Engine INPOL

DE 200 16 748 U1

104b Search Engine EUROPOL

105a Antwort INPOL

105b Antwort EUROPOL

106 Rückmeldung an PM Zabel

107 Erfassung des Sachbestands

108a Sicherung von Daten/Metadaten

108b Generierung Standardbericht

109 Standardbericht und Daten an Dienstleiter

110a Funkkontakt zwischen PM Zabel und Dienstleister

110b Anweisungen des Dienstleiters an POM Sicher und PM Zabel

111a Abonnement-Engine Tagesauswertung

111b Erzeugung der Tagesauswertung

111c Tagesauswertung an Dienstleiter

112a Weitere Einsatzplanung

DE 200 16 746 U1

## 112b Sicherung der Einsatzplanung

Die in der vorstehenden Beschreibung, in den Zeichnungen sowie in den Ansprüchen offenbarten Merkmale der Erfindung können sowohl einzeln als auch in beliebigen Kombinationen für die Verwirklichung der Erfindung in ihren verschiedenen Ausführungsformen wesentlich sein.

DE 200 16 746 U1

Bezugszeichenliste

10 – 16	Endgeräte
17	Kommunikationseinrichtungen
18	Datenfernübertragungseinrichtungen
20	Router
22	HTTP-Server
24	WAP-Server
26	Datenfernübertragungseinrichtung
28	IVR-Server
30, 32	Firewall machine
34	Applikations-Server
36, 36a, 36b, 36c, 36d	Externe Datenbank
38	Router
40	WAN
42	Lokale Einrichtung für eine Applikation
43	Lokale Media-Datenbank
44	Lokales Bürokommunikationssystem
45	Lokale Datenbank
46	Lokales Data Warehouse
48	Drucker
50, 52	Benutzer

Bezugszeichenliste

10 – 16	Endgeräte
17	Kommunikationseinrichtungen
18	Datenfernübertragungseinrichtungen
20	Router
22	HTTP-Server
24	WAP-Server
26	Datenfernübertragungseinrichtung
28	IVR-Server
30, 32	Firewall machine
34	Applikations-Server
36, 36a, 36b, 36c, 36d	Externe Datenbank
38	Router
40	WAN
42	Lokale Einrichtung für eine Applikation
43	Lokale Media-Datenbank
44	Lokales Bürokommunikationssystem
45	Lokale Datenbank
46	Lokales Data Warehouse
48	Drucker
50, 52	Benutzer

54	Einrichtung zur Authentifizierung und Identifizierung
56	Abonnement-Engine
58	Filter-Engine
60	Information Repository-Engine
62	Application Repository-Engine
64	Office Communication Repository-Engine
66	Mehrwertdienst
67	Schnittstellen-Integrator
68	Request Broker
70	Output-Engine
101	Authentifizierung
102a	Personalisierung
102b	Darstellung des Portals
103	Suchabfrage Kennzeichen
104a	Search Engine INPOL
104b	Search Engine EUROPOL
105a	Antwort INPOL
105b	Antwort EUROPOL
106	Rückmeldung an PM Zabel
107	Erfassung des Sachbestands
108a	Sicherung von Daten/Metadaten
108b	Generierung Standardbericht
109	Standardbericht und Daten an Dienstleiter
110a	Funkkontakt zwischen PM Zabel und Dienstleister
110b	Anweisungen des Dienstleiters an POM Sicher und PM

-3- 28.09.00

Zabel

111a	Abonnement-Engine Tagesauswertung
111b	Erzeugung der Tagesauswertung
111c	Tagesauswertung an Dienstleiter
112a	Weitere Einsatzplanung
112b	Sicherung der Einsatzplanung
A	Zugangskanäle
B	Portal
C	Nachgelagerte Informationssysteme
DL	Dienststellenleiter
DS	Dienststelle
PVB	Polizeivollzugsbeamter

DE 200 16 746 U1

28.09.00

# BOEHMERT & BOEHMERT ANWALTSSOZietät

Boehmert & Boehmert - P.O.B. 10 71 27 - D-28071 Bremen

Deutsches Patent- und Markenamt  
Zweibrückenstr. 12

80297 München

DR.-ING. KARL BOEHMERT, PA (1899-1973)  
DIPL.-ING. ALBERT BOEHMERT, PA (1902-1993)  
WILHELM J. H. STAHLBERG, RA, Bremen  
DR.-ING. WALTER HOORMANN, PA\*, Bremen  
DIPL.-PHYS. DR. HEINZ GODDAR, PA\*, München  
DR.-ING. ROLAND LIESEGANG, PA\*, München  
WOLF-DIETER KUNTZE, RA, Bremen, Alicante  
DIPL.-PHYS. ROBERT MÜNZHUBER, PA (1933-1992)  
DR. LUDWIG KOUKER, RA, Bremen  
DR. (CHEM.) ANDREAS WINKLER, PA\*, Bremen  
MICHAELA HUTH-DIERIG, RA, München  
DIPL.-PHYS. DR. MARION TÖNHARDT, PA\*, Düsseldorf  
DR. ANDREAS EBERT-WEIDENFELLER, RA, Bremen  
DIPL.-ING. EVA LIESEGANG, PA\*, München  
DR. AXEL NORDEMANN, RA, Berlin  
DIPL.-PHYS. DR. DOROTHÉE WEBER-BRULS, PA\*, Frankfurt  
DIPL.-PHYS. DR. STEFAN SCHOHE, PA\*, München  
DR.-ING. MATTHIAS PHILIPP, PA\*, Bielefeld  
DR. JAN BERND NORDEMANN, LL.M., RA, Berlin

PROF. DR. WILHELM NORDEMANN, RA, B&B  
DIPL.-PHYS. EDUARD BAUMANN, PA\*, Hehenkirchen  
DR.-ING. GERALD KLÖPSCH, PA\*, Düsseldorf  
DIPL.-ING. HANS W. GROENING, PA\*, München  
DIPL.-PHYS. SIEGFRIED SCHIRMER, PA\*, Bielefeld  
DIPL.-PHYS. LORENZ HANEWINKEL, PA\*, Paderborn  
DIPL.-ING. DR. JAN TÖNNIES, PA, RA, Kiel  
DIPL.-PHYS. CHRISTIAN BIEHL, PA\*, Kiel  
MARTIN WIRTZ, RA, Düsseldorf  
DR. DETMAR SCHÄFER, RA, Bremen  
DIPL.-PHYS. DR.-ING. UWE MANASSE, PA\*, Bremen  
DR. CHRISTIAN CZYCHOWSKI, RA, Berlin  
DR. CARL-RICHARD HAARMANN, RA, München  
DIPL.-PHYS. DR. THOMAS L. BITTNER, PA\*, Berlin  
DR. VOLKER SCHMITZ, RA, München  
DR. FRIEDRICH NICOLAUS HEISE, RA, Potsdam  
DIPL.-PHYS. CHRISTIAN W. APPELT, PA, München  
DR. ANKE NORDEMANN-SCHIFFEL, RA\*, Potsdam  
KERSTIN MAUCH, LL.M., RA, Potsdam

In Zusammenarbeit mit/in cooperation with  
DIPL.-CHEM. DR. HANS ULRICH MAY, PA\*, München

PA - Patentanwalt/Patent Attorney  
RA - Rechtsanwalt/Attorney at Law  
\* - European Patent Attorney  
• - Brandenburg, zugelassen am OLG Brandenburg  
o - Maître en Droit  
Alle zugelassen zur Vertretung vor dem Europäischen Patentamt, Alicante  
Professional Representatives at the Community Trademark Office, Alicante

Ihr Zeichen  
Your ref.

Ihr Schreiben  
Your letter of

Unser Zeichen  
Our ref.

Bremen,

Anmeldung  
Gebrauchsmuster

A10026

27. September 2000

Andersen Cosulting Unternehmensberatung GmbH, Otto-Vogler-Straße 15, 65843 Sulzbach  
"Informationsdienstssystem"

## Ansprüche

1. Informationsdienstsystem mit Applikationseinrichtungen, insbesondere für die Polizei,

mit

- Informationssystemen (C),

- 28.73 -

Hollerallee 32 - D-28209 Bremen - P.O.B. 10 71 27 - D-28071 Bremen - Telefon +49-421-34090 - Telefax +49-421-3491768

MÜNCHEN - BREMEN - BERLIN - DÜSSELDORF - FRANKFURT - BIELEFELD - POTSDAM - BRANDENBURG - KIEL - PADERBORN - HÖHENKIRCHEN - ALICANTE

http://www.boehmert.de e-mail: postmaster@boehmert.de



- einem intelligenten, dynamisch realisierten Portal (B) für einen einheitlichen Zugang zu den nachgelagerten Informationssystemen (C) mit einem vom Benutzer abhängigen Umfang,
  - mindestens einem Endgerät (10; 12; 14; 16) für einen Zugang zu dem Portal (B), und
  - mindestens einer Kommunikationseinrichtung (17) zum Verbinden des Endgeräts (10, 12, 14, 16) mit dem Portal.
2. Informationsdienstsystem nach Anspruch 1, dadurch gekennzeichnet, daß die Informationssysteme (C) mindestens eine externe (36; 36a; 36b; 36c; 36d) und/oder mindestens eine lokale Datenbank (45) umfassen.
  3. Informationsdienstsystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Informationssysteme (C) mindestens eine lokale Media-Datenbank (43) umfassen.
  4. Informationsdienstsystem nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Informationssysteme (C) mindestens ein lokales Data Warehouse (46) umfassen.
  5. Informationsdienstsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Informationssysteme (C) mindestens eine lokale Einrichtung (42) für eine Applikation umfassen.
  6. Informationsdienstsystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Informationssysteme (C) mindestens ein lokales Bürokommunikationssystem (44) umfassen.

DE 200 16 746 U1

7. Informationssystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das Portal (B) einen Server umfaßt.
8. Informationssystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das Portal (B) eine Engine- Schicht mit mindestens einer Engine auf einer Schicht mit einer Administrationseinrichtung zur Verwaltung von Benutzern, Konfiguration der Engine(s) und Administration von vor- und nachgelagerten Schichten umfaßt.
9. Informationssystem nach Anspruch 7 oder 8, dadurch gekennzeichnet, daß das Portal (B) in einer vorgelagerten Schicht eine Einrichtung (54) zur Authentifizierung eines Benutzers und des Servers umfaßt.
10. Informationssystem nach Anspruch 9, dadurch gekennzeichnet, daß die Einrichtung zur Authentifizierung eine Einrichtung zur Identifizierung eines Benutzers umfaßt.
11. Informationssystem nach Anspruch 9 oder 10, dadurch gekennzeichnet, daß das Portal in der vorgelagerten Schicht eine Autorisierungssteuer- und eine -speichereinrichtung zur Regelung des Umfangs des Zugangs eines Benutzers umfaßt.
12. Informationssystem nach Anspruch 11, dadurch gekennzeichnet, daß das Portal (B) eine Einrichtung zur Darstellung der Nutzungsmöglichkeiten des Portals in Abhängigkeit vom äußeren Kontext, wie z. B. Datum, Tageszeit, Benutzer, besondere Vorkommnisse, aufweist.
13. Informationssystem nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, daß das Portal in der vorgelagerten Schicht eine Einrichtung zur Verschlüsselung der über die Kommunikationseinrichtung (17) gesendeten Daten und zur Entschlüsselung der über die Kommunikationseinrichtung (17) empfangenen Daten umfaßt.

DE 200 16 746 U1

14. Informationssystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das Portal (B) eine Einrichtung zur Wahrung bzw. Feststellung der Integrität der über die Kommunikationseinrichtung (17) gesendeten und empfangenen Daten umfaßt.
15. Informationssystem nach einem der Ansprüche 8 bis 14, dadurch gekennzeichnet, daß die Engine-Schicht eine Abonnement-Engine (56) zum Abonnieren von Informationen Verzeichnissen und weiteren Diensten durch einen Benutzer umfaßt.
16. Informationssystem nach einem der Ansprüche 8 bis 15, dadurch gekennzeichnet, daß die Engine-Schicht eine Filter-Engine (58) umfaßt.
17. Informationssystem nach einem der Ansprüche 8 bis 16, dadurch gekennzeichnet, daß die Engine-Schicht eine Information Repository-Engine (60) und/oder eine Application Repository-Engine (62) und/oder eine Office Communication Repository-Engine (64) umfaßt.
18. Informationssystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das Portal (B) eine Output-Engine (70) umfaßt.
19. Informationssystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das Portal (B) einen Schnittstellen-Integrator (67) für die nachgelagerten Informationssysteme (C) umfaßt.
20. Informationssystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das Portal (B) mindestens ein Mehrwertdienstsystem (66) umfaßt.
21. Informationssystem nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das Portal (B) einen Request Broker (68) umfaßt.

DE 200 16 748 U1

22. Informationssystem nach einem der vorangehenden Ansprüche, gekennzeichnet durch eine Firewall machine (30) zwischen dem Portal (B) und der mindestens einen Kommunikationseinrichtung (17).
23. Informationssystem nach einem der vorangehenden Ansprüche, gekennzeichnet durch eine Firewall machine (32) zwischen dem Portal (B) und den nachgelagerten Informationssystemen (C).

DE 200 16 746 U1

08.11.00

1 / 3

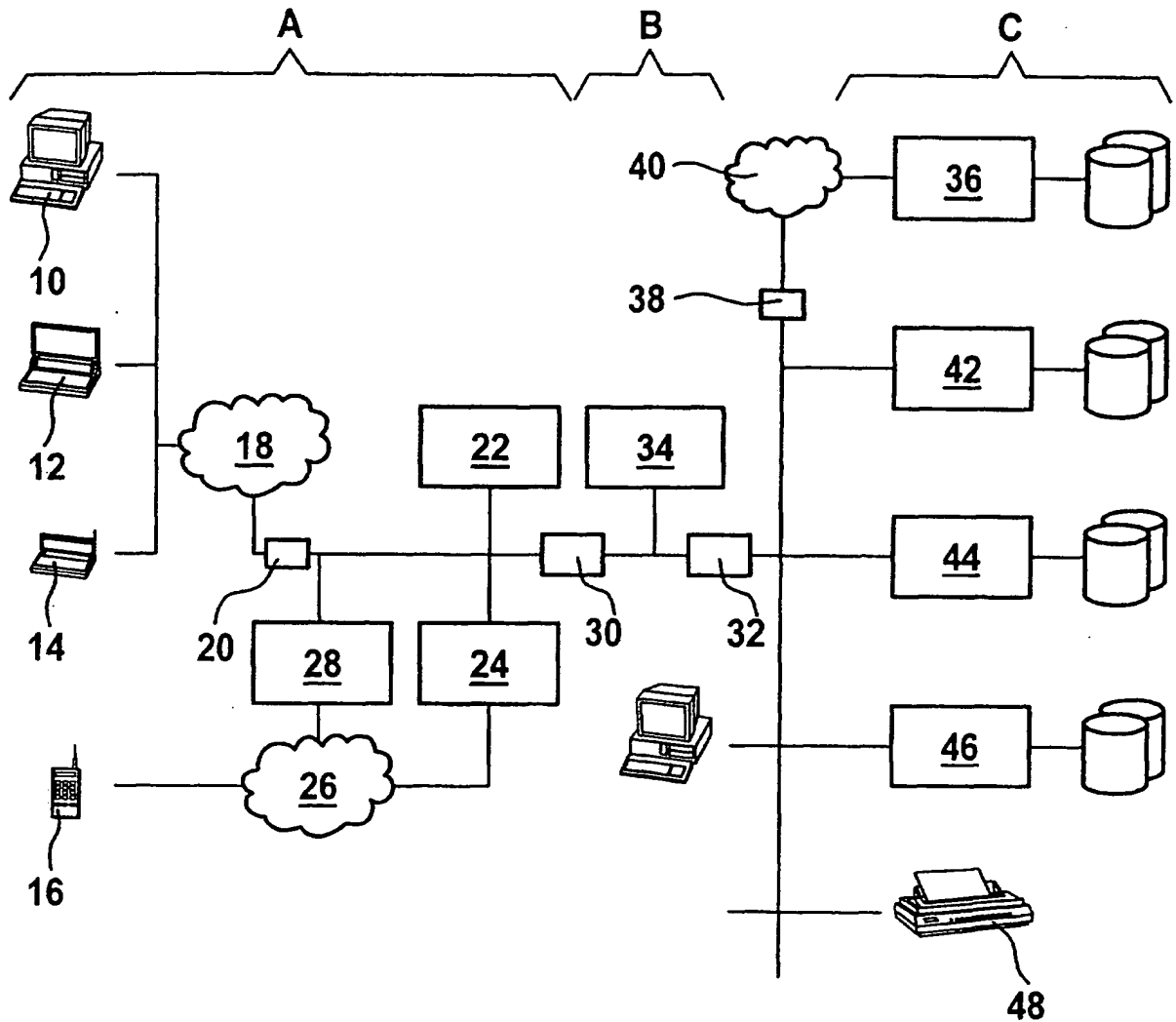


Fig. 1

DE 200 16 746 U1

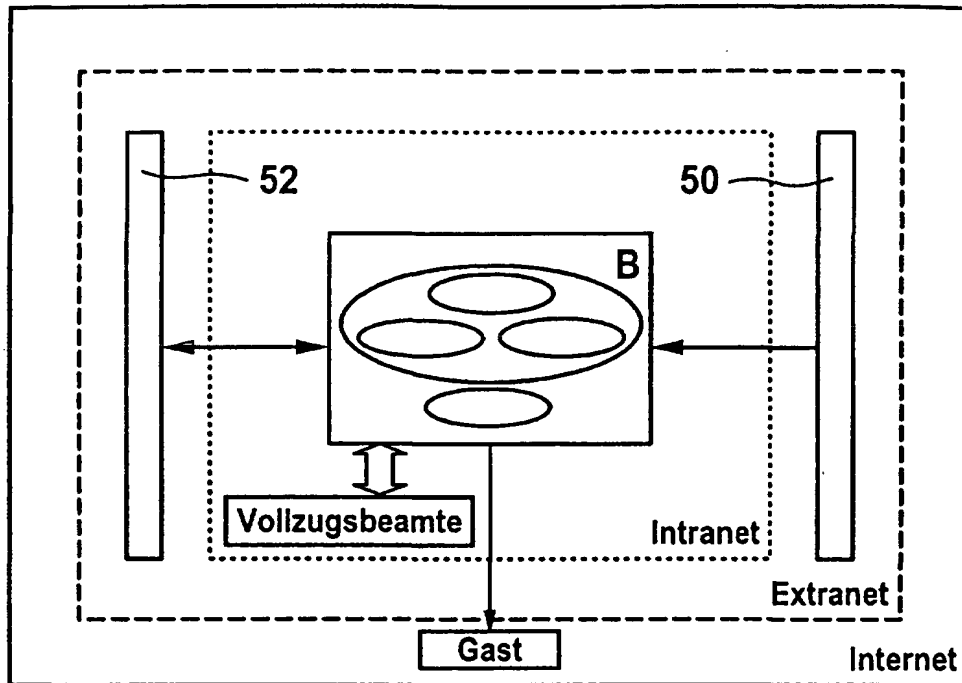


Fig. 2

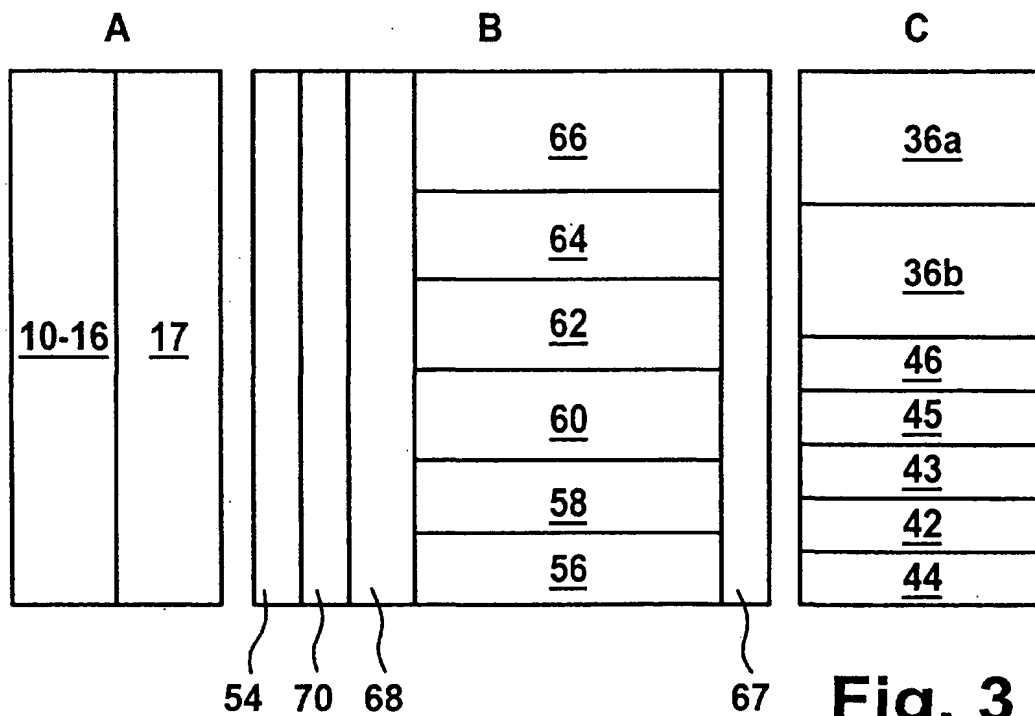


Fig. 3

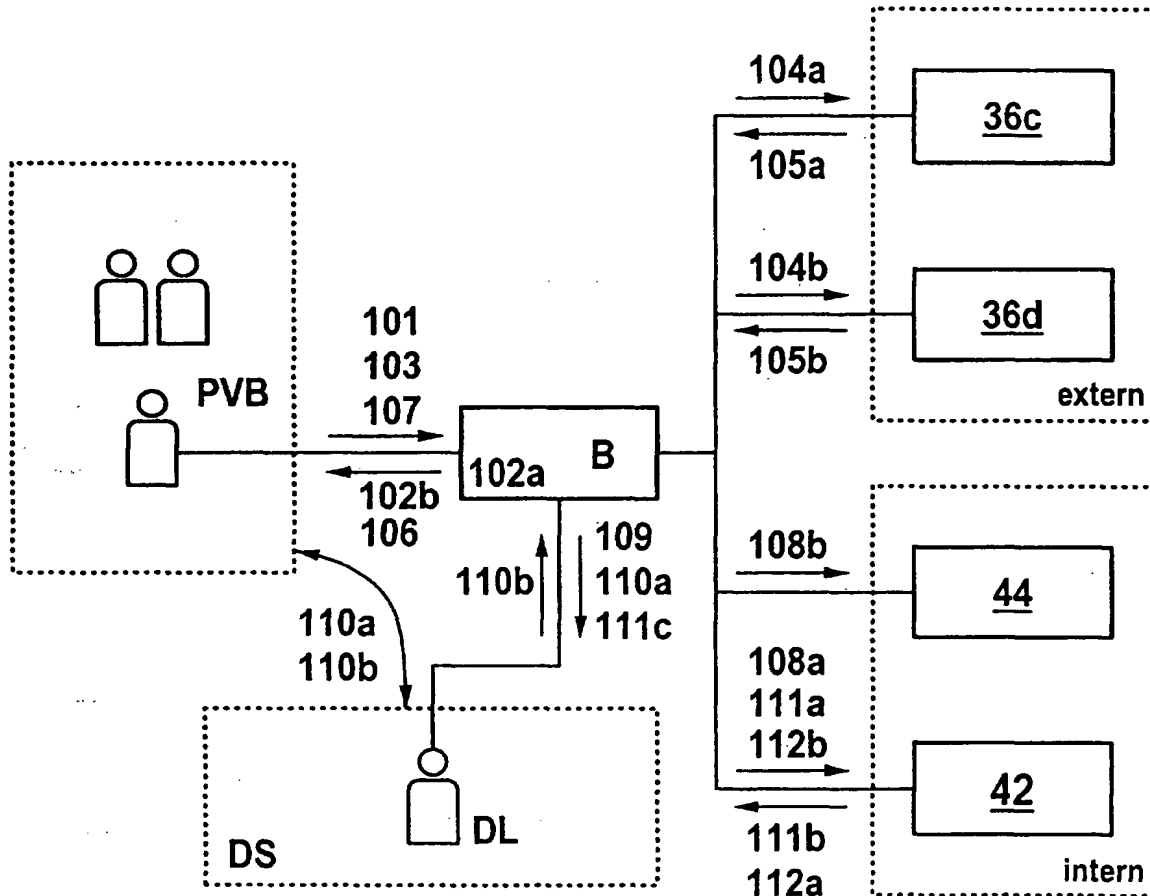


Fig. 4